Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1.   (Currently Amended) A scalable on-line system for printing value bearing items (VBI) comprising:

a client system; and

a scalable server system communicating with the client system over a communication network comprising:

a database remote from the client system and including information about a plurality of users;

a plurality of ~~security device~~ transaction data records stored in the database to ensure authenticity of the plurality of users, wherein ~~the scalable server system is configured to process each security device transaction data record in a stateless manner~~ each transaction data record includes information to restore the data record to its last known state, when the data record is next used; and

a plurality of stateless cryptographic ~~module to authenticate~~ devices remote from the client system and capable of authenticating and processing VBI printing requests from any of the plurality of users using a respective ~~one or more of the plurality of security device~~ transaction data records stored in the database, ~~in a stateless manner~~ wherein when a VBI printing request from a current user is received by the server system, an available cryptographic device from the plurality of cryptographic devices loads the current user's transaction data record and instantiates a user state in the transaction data record to process the VBI printing requests from the current user.

2.   (Currently Amended) The scalable on-line system of claim 1, wherein each ~~security device~~ transaction data record is related to a user.

3.   (Currently Amended) The scalable on-line system of claim 2, wherein the ~~security device~~ transaction data record related to a user is loaded into ~~the~~ <u>a respective</u> cryptographic module when the user requests to operate on a value bearing item.

4.   (Currently Amended) The scalable on-line system of claim 3, wherein the ~~security device~~ transaction data record related to a user is updated and returned to the database.

5. - 7. (Cancelled)

8.   (Currently Amended) The scalable on-line system of claim [[5]] <u>1</u>, further comprising computer executable code for load-balancing to distribute traffic among multiple cryptographic modules.

9.   (Cancelled)

10.   (Previously Presented) The scalable on-line system of claim 1, wherein the database is partitioned across a plurality of physical databases.

11.   (Currently Amended) The scalable on-line system of claim 1, wherein ~~the~~ <u>each</u> cryptographic ~~module~~ <u>device</u> performs cryptographic function on a transaction related to the database.

12.   (Previously Presented) The scalable on-line system of claim 1, further comprising computer executable code for password authentication to prevent unauthorized access to the database.

13.   (Currently Amended)   The scalable on-line system of claim 1, wherein the database stores a first set of one or more last database transactions and ~~the~~ each cryptographic ~~module~~ device stores a second set of one or more last database transactions for comparison with the first set of one or more last database transactions stored in the database to verify each database transaction.

14.   (Currently Amended)   The scalable on-line system of claim 13, wherein ~~the~~ each cryptographic ~~module~~ device prevents further database transactions if the second set of one or more last transaction stored in the cryptographic module does not compare with the first set of one or more last transaction stored in the database.

15.   (Currently Amended)   The scalable on-line system of claim 1, wherein each cryptographic ~~module~~ device includes a data validation subsystem for allowing the module to verify that data is up to date and an auto-recovery subsystem for automatically re-synchronize the module with the data.

16.   (Currently Amended)   The scalable on-line system of claim 1, wherein ~~the~~ each cryptographic ~~module~~ device includes a computer executable code for preventing unauthorized modification of data.

17.   (Currently Amended)   The scalable on-line system of claim 1, wherein ~~the~~ each cryptographic ~~module~~ device includes a computer executable code for ensuring proper operation of cryptographic security and VBI related meter functions.

18.   (Currently Amended)   The scalable on-line system of claim 1, wherein ~~the~~ each cryptographic ~~module~~ device includes a computer executable code for supporting multiple concurrent users.

-4-

19.   (Previously Presented)   The scalable on-line system of claim 1, wherein the database includes one or more indicium data elements, data for account maintenance, and data for revenue protection.

20.   (Previously Presented)   The scalable on-line system of claim 1, wherein the database includes virtual meter information.

21.   (Previously Presented)   The scalable on-line system of claim 1, wherein the database includes descending register data.

22.   (Previously Presented)   The scalable on-line system of claim 1, wherein the value bearing item is a mail piece.

23.   (Previously Presented)   The scalable on-line system of claim 22, wherein postal indicium comprises a digital signature.

24.   (Currently Amended)   The scalable on-line system of claim 1, wherein ~~the~~ a respective cryptographic ~~module~~ device performs cryptographic function on validation information according to a user request for printing a VBI.

25.   (Currently Amended)   The scalable on-line system of claim 1, wherein ~~the~~ a respective cryptographic ~~module~~ device generates data sufficient to print a postal indicium in compliance with postal service regulation on a mail piece.

26.   (Previously Presented)   The scalable on-line system of claim 1, wherein the value bearing item is a ticket.

27.   (Previously Presented)   The scalable on-line system of claim 1, wherein a bar code is printed on the value bearing item.

28.   (Previously Presented)   The scalable on-line system of claim 1, wherein the value bearing item is a coupon.

29.   (Previously Presented)   The scalable on-line system of claim 1, wherein the value bearing item is currency.

30.   (Previously Presented)   The scalable on-line system of claim 1, wherein the value bearing item is a voucher.

31.   (Previously Presented)   The scalable on-line system of claim 1, wherein the value bearing item is a traveler's check.

32.   (Currently Amended)   The scalable on-line system of claim 1, wherein each security device transaction data record includes one or more of an ascending register value, a descending register value, a respective cryptographic module ID, an indicium key certificate serial number, a licensing ZIP code, a key token for an indicium signing key, user secrets, a key for encrypting user secrets, date and time of last transaction, last challenge received from a respective client subsystem, an operational state of the respective module, expiration dates for keys, and a passphrase repetition list.

33.   (Currently Amended)   The scalable on-line system of claim 1, wherein each security device transaction data record includes one or more of a private key, a public key, and a public key certificate, wherein the private key is used to sign module status responses and a VBI which, in conjunction with a public key certificate, demonstrates that the module and the VBI are authentic.

34.　(Currently Amended)　The scalable on-line system of claim 1, wherein ~~the~~ each cryptographic module includes executable instructions to perform one or more of Rivest, Shamir and Adleman (RSA) public key encryption, DES, Triple-DES, DSA signature, SHA-1, and Pseudo-random number generation algorithms.

35.　(Previously Presented)　The scalable on-line system of claim 1, wherein the server system further comprises one or more of a postal server subsystem, a provider server subsystem, an e-commerce subsystem, a staging subsystem, a client support subsystem, a decision support subsystem, a SMTP subsystem, an address matching service subsystem, a SSL proxy server subsystem, and a web server subsystem.

36.　(Previously Presented)　The scalable on-line system of claim 1, wherein the database includes one or more of a postal database, a provider database, an e-commerce database, and a membership database.

37.　(Previously Presented)　The scalable on-line system of claim 1, further comprising an address matching server for verifying a correct address specified by a user.

38.　(Previously Presented)　The scalable on-line system of claim 1, further comprising a printer driver database for storing supported printer driver information.

39.　(Currently Amended)　A method for printing value-bearing items (VBI) via a communication network including a client system, and a server system, the method comprising the steps of:

　　　accepting print requests from a plurality of users by the client system;
　　　communicating the print requests to the server system over the communication network;

storing in a database a plurality of ~~security device~~ transaction data records, wherein each transaction data record includes information to restore the data record to its last known state, when the data record is next used;

ensuring authenticity of the plurality of users utilizing a respective ~~security device~~ transaction data record;

processing in a stateless manner each ~~security device~~ transaction data record in the server system;~~and~~

authenticating by a ~~scalable~~ cryptographic ~~module~~ device any of the plurality of users in a stateless manner, utilizing one or more of the plurality of ~~security device~~ transaction data record stored in the database;

receiving a VBI printing request from a current user;

loading the current user's transaction data record in the cryptographic device; and

instantiating a user state in the transaction data record to process the VBI printing requests from the current user.

40. (Currently Amended) The method of claim 39, wherein each ~~security device~~ transaction data record is related to a user.

41. (Canceled)

42. (Currently Amended) The method of claim [[41]]39, further comprising the steps of updating and returning the ~~security device~~ transaction data record related to a user to the database.

43. (Currently Amended) The method of claim 39, further comprising the step of adding at least one more ~~stateless~~ cryptographic ~~module~~ device, wherein each cryptographic ~~module~~ device is capable of processing any of the plurality of ~~security device~~ transaction data records.

44.   (Currently Amended)   The method of claim 39, further comprising the step of authenticating a user using any of the cryptographic ~~modules~~ <u>devices</u>.

45.   (Currently Amended)   The method of claim 43, further comprising the step of load-balancing to route user requests to the at least one more cryptographic ~~module~~ <u>device</u>.

46.   (Currently Amended)   The method of claim 43, further comprising the step of load-balancing to distribute traffic among the multiple cryptographic ~~modules~~ <u>devices</u>.

47.   (Original)   The method of claim 39, further comprising the step of the authenticating any of the one or more users using the cryptographic module.

48.   (Original)   The system of claim 1, further comprising the step of partitioning the database across a plurality of physical databases.

49.   (Currently Amended)   The method of claim 39, further comprising the step of encrypting database transactions using the cryptographic ~~module~~ <u>device</u>.

50.   (Original)   The method of claim 39, further comprising the steps of verifying a user password before granting access to the database.

51.   (Currently Amended)   The method of claim 39, further comprising the steps of
storing one or more last database transactions in the database;
storing one or more last database transactions in the cryptographic ~~module~~ <u>device</u>; and
comparing the one or more last database transactions stored in the database with the one or more last database transactions stored in the cryptographic ~~module~~ <u>device</u> to verify each database transaction.

52.   (Currently Amended)   The method of claim 39, further comprising the step of encrypting transactions related to the database using the cryptographic ~~module~~ device.

53.   (Currently Amended)   The method of claim 39, further comprising the steps of storing one or more last database transactions in the database, storing one or more last database transactions in the cryptographic ~~module~~ device for comparison with the one or more last database transactions stored in the database to verify each database transaction.

54.   (Currently Amended)   The method of claim 53, further comprising the step of preventing further database transactions if the one or more last transaction stored in the cryptographic ~~module~~ device does not compare with the one or more last transaction stored in the database.

55.   (Currently Amended)   The method of claim 39, further comprising the steps of preventing unauthorized modification of data using the cryptographic ~~module~~ device.

56.   (Original)   The method of claim 39, further comprising the steps of verifying that the database is up to date.

57.   (Currently Amended)   The method of claim 39, further comprising the steps of automatically re-synchronizing the cryptographic ~~module~~ device with the database.

58.   (Previously Presented)   The method of claim 39, further comprising the step of ensuring proper operation of cryptographic security and VBI related meter functions.

59.   (Original)   The method of claim 39, further comprising the steps of supporting multiple concurrent operators.

60.   (Currently Amended) The method of claim [[39]]43, further comprising the steps of:

storing information about a number of last transactions in a respective internal register of each of the ~~one or more~~ cryptographic devices;

storing a table including the information about a last transaction in the database;

comparing the information saved in the respective device with the respective information saved in the database; and

loading a new transaction data if the respective information stored in the device compares with the respective information stored in the database.

61.   (Original) The method of claim 39, further comprising the step of storing data for creating one or more indicium, account maintenance, and revenue protection.

62.   (Original) The method of claim 39, further comprising the step of printing a mail piece.

63.   (Original) The method of claim 62, wherein the mail piece includes a digital signature.

64.   (Original) The method of claim 62, wherein the mail piece includes a postage amount.

65.   (Original) The method of claim 62, wherein the mail piece includes an ascending register of used postage and descending register of available postage.

66.   (Original) The method of claim 50, further comprising the step of printing a ticket.

67.   (Original) The method of claim 39, further comprising the step of printing a bar code.

68.   (Original) The method of claim 39, further comprising the step of printing a coupon.

69.   (Original) The method of claim 39, further comprising the step of printing currency.

70.   (Original) The method of claim 39, further comprising the step of printing a voucher.

71.   (Original) The method of claim 39, further comprising the step of printing a traveler's check.

72.   (Currently Amended) The method of claim 39, wherein each of the ~~security device~~ transaction data records includes an ascending register value, a descending register value, a respective cryptographic device ID, an indicium key certificate serial number, a licensing ZIP code, a key token for an indicium signing key, user secrets, a key for encrypting user secrets, date and time of last transaction, last challenge received from a respective client subsystem, an operational state of the respective device, expiration dates for keys, and a passphrase repetition list.

73.   (Currently Amended) The method of claim 39, further comprising the step of performing one or more of Rivest, Shamir and Adleman (RSA) public key encryption, DES, Triple-DES, DSA signature, SHA-1, and Pseudo-random number generation algorithms using ~~each of~~ the cryptographic ~~devices~~ device.

74. (Original) The method of claim 39, further comprising the step keeping track of user accesses to a vendor website using a website database.

75. (Original) The method of claim 39, further comprising the step of storing postal transaction data, financial transaction data, customer marketing information, commerce product information, meter license information, meter resets, meter history, and meter movement information in an offline database.

76. (Original) The method of claim 39, further comprising the step of storing customer information, financial transactions, and information for marketing queries in a data warehouse database.

77. (Original) The method of claim 39, further comprising the steps of authorizing and capturing funds from a customer's account and transferring the funds to a vendor's account using an e-commerce server.

78. (Original) The method of claim 39, further comprising the step of verifying a correct address specified using a user using an address matching server.

79. (Original) The method of claim 39, further comprising the step of storing supported printer driver information in a printer driver database.